

Before the Federal Communications Commission

In the matter of:

PUBLIC SAFETY AND HOMELAND SECURITY BUREAU SEEKS COMMENT ON
PETITIONS FILED BY THE BOULDER REGIONAL EMERGENCY TELEPHONE
SERVICE AUTHORITY

PS Docket 19-254

Specifically, FirstNet Prioritized Public Safety Interoperability with Commercial Carriers, and Commission Rulemaking under US Code 47 CFR 1431 “Public safety roaming and priority access”

State of Illinois Public Safety Broadband Working Group (Illinois)

The State of Illinois is an enthusiastic supporter of the FirstNet project. We have reached the point where advanced LTE technology has been harnessed to provide Public Safety with the communications tools they need to protect and serve the citizens of the United States. The requirement of LTE standard-based priority and preemption is arguably the single most important feature available to Public Safety. The work of AT&T and FirstNet on this project to date has been remarkable.

However, we see disturbing parallels between the current lack of prioritized interoperability between carriers and the history of interoperability (or lack thereof) between proprietary digital Land Mobile Radio (LMR) systems. For decades, Public Safety has struggled, and still struggles with interoperability because of incompatible LMR systems, and we see the same problems ahead with the way FirstNet currently works with the other cellular carriers.

For this reason, Illinois supports the petition filed by the Boulder Regional Emergency Telephone Service Authority (BRETSA), as well as many other commenters. We believe that it will be in the public interest for the Commission to develop rules to enhance the ability of Public Safety to communicate seamlessly between the FirstNet network and other carriers offering Public Safety communications services. Our sole priority is to ensure the ability of responders to communicate with each other without regard to which carrier network they may be using.

Illinois believes the Commission is empowered to, and should, act on this issue pursuant to US Code, Title 47, Chapter 13, Subchapter II, 1431:

§ 1431. Public safety roaming and priority access

The Commission may adopt rules, if necessary in the public interest, to improve the ability of public safety networks to roam onto commercial networks and to gain priority access to commercial networks in an emergency if—

(1) the public safety entity equipment is technically compatible with the commercial network;

(2) the commercial network is reasonably compensated; and

(3) such access does not preempt or otherwise terminate or degrade all existing voice conversations or data sessions.

(Pub. L. 112–96, title VI, § 6211, Feb. 22, 2012, 126 Stat. 218.)

Summary of Comments:

We believe that it is in the public interest that the Commission, in order to foster true Public Safety Grade inter-network communications interoperability for Public Safety, should adopt rules that will require:

- Public Safety users on any carrier's Long Term Evolution (LTE) network that have Public Safety grade Quality of Service, Priority, and Preemption (QPP) to be able to communicate with Public Safety users on any application, on any other carrier's network, including FirstNet, while maintaining their QPP status across networks.
- Public Safety responders using Mission Critical Push to Talk (MC-PTT) services that follow the applicable 3rd Generation Partnership Project (3GPP) LTE standards on any carrier's network, should be able to seamlessly communicate via MC-PTT to users on any other Public Safety carrier network(s) supplying Public Safety MC-PTT services that also follow the applicable 3GPP LTE standards.
- Public Safety user devices to be able to roam between FirstNet and any other carrier's network as needed and as authorized by the Public Safety agency, and be able to communicate with Public Safety QPP settings on any network.
- And encourage greater competition in the Public Safety broadband arena that will encourage innovation, efficiency, and cost savings for Public Safety agencies.

We believe that First Responders using any cellular network (including FirstNet) should have the benefit of prioritized emergency communications with First Responders using any other cellular network, without concern as to the source of that network service.

MC-PTT is the primary tactical communications method for on-scene responders. This prioritization issue is especially critical if carriers intend to provide and promote Public Safety use of MC-PTT over the carriers' LTE based networks as a viable option for replacing their existing Land Mobile Radio (LMR) networks.

And, because tactical MC-PTT voice communications are so critical to the ability of emergency responders to protect the life and safety of our citizens, responders using cellular MC-PTT need to be able to communicate seamlessly with other responders, without having to worry about which network they happen to be using.

We are of the opinion that live video streams from responders are an important tool that will reshape how Public Safety operates. Prioritization of those video streams is a key element in the reliability and stability of the delivered video. However, the loss of prioritization, which could constrict the free flow of those streams during transfer between

carriers, means that the use of video could become difficult, if not impossible, in an emergency situation.

Based on our reading of both the “Middle Class Tax Relief and Job Creation Act of 2012” and the relevant sections for FirstNet of US Code, Title 47, Chapter 13, Subchapter II, we believe that Congress intended that there be seamless interoperability for emergency responders between the FirstNet network and commercial cellular networks, no matter if FirstNet was built from the ground up, or supplied as a service by a carrier.

Prioritized, seamless interoperable communications between carriers, i.e., MC-PTT or Mission Critical Video communications, while maintaining Public Safety Quality of Service, Priority, and Preemption (QPP) status regardless of carrier, are an absolute necessity for Public Safety.

Introduction

As stated earlier, the State of Illinois is a supporter of the FirstNet project. We believe that Public Safety needs dedicated, prioritized, broadband cellular service in order to fully serve and protect their citizens. We are enthusiastic at the prospect of securing the ability to send data and video in an emergency situation, free from the congestion that impairs the ability of emergency responders to use the commercial networks. We feel that FirstNet’s requirement of LTE standard-based priority and preemption is arguably the single most important feature available to Public Safety.

We recognize the First Responder Network Authority for their tireless efforts which have led to the incredible progress we see in the National Public Safety Broadband Network today.

However, we feel that Public Safety use of Carrier LTE networks & services can be greatly improved. Therefore, Illinois supports the petition filed by the Boulder Regional Emergency Telephone Service Authority (BRETSA). We believe that it will be in the public interest for the Commission to develop rules to enhance the ability of Public Safety to communicate seamlessly between the FirstNet network and other carriers offering Public Safety communications services. Our sole priority is to ensure the ability of responders to communicate with each other without regard to which carrier network they may be using.

We also support the Colorado Public Safety Broadband Governing Body’s (CPSBGB) July 6, 2018 filing requesting the Commission to clarify guidelines and requirements for interoperability and roaming between the NPSBN and other commercial wireless networks. We believe they raised some very important issues that should be explored in a rulemaking process.

We note and agree in principle with the National Public Safety Telecommunications Council’s (NPSTC) Position Statement on FirstNet. However, from an interoperable MC-PTT perspective, the current situation is that of users on multiple carrier networks being able to communicate via PTT, at least without extra interoperability equipment. We

believe that the 3GPP LTE standards provide for different carriers networks to appear as a single network to the users, and boundaries or divisions between the networks would be invisible to the user. This would give Public Safety what it really needs: MC-PTT users from any agency, on any carrier to interoperate seamlessly with each other.

Our citizens demand, and deserve, the most reliable, efficient and expedient Public Safety service possible. Intra-agency and interoperable communications are absolutely critical to Public Safety in this mission. However, we are concerned with the direction that the project seems to be heading, specifically in the areas of competition and interoperability.

From a Land Mobile Radio (LMR) perspective, Public Safety has fought for decades for the ability of radios and systems to interoperate all the way down to the individual radio level. As digital LMR systems began to proliferate, there were (and still are) proprietary systems, and some manufacturers had no interest in supporting true interoperability. Additionally, with proprietary systems, once an agency chooses a particular system they are locked in to that manufacturer for the life of the system. This has obvious financial consequences for agencies and our taxpayers, as they expect Public Safety to provide services in the most fiscally efficient manner.

True interoperability was considered a minor item, and supported only as long as it did not affect market share and the bottom line. Public Safety saw that this was an untenable situation, and worked diligently to drive the philosophy of interoperability, and standards to support it. An excellent example of this are the APCO Project 25 standards that require that radio systems be able to interoperate at multiple levels, regardless of manufacturer or vendor.

In the LMR world today, interoperability is still a struggle, but we are grateful that the manufacturers are adopting the philosophy and standards, and the technology supports interoperability more and more with each new version in LMR.

We are concerned and disappointed that FirstNet seems to be falling into the same trap that the Public Safety LMR community had begun to address almost 30 years ago, specifically proprietary systems and networks. One critical concern is that even if all carriers use the exact same LTE standard for MC-PTT, they will not allow the connections between networks required for seamless MC-PTT between different Public Safety agencies to occur, regardless of carrier.

Another concern is what appears to us to be arbitrary restrictions on allowing prioritized data transfer between First Responders who may happen to be using different carrier networks. This issue affects not only MC-PTT, but could affect all other types of communications between responders on different networks.

We are very concerned that carriers, vendors, and manufacturers, in spite of Public Safety's efforts to educate them on our needs, simply do not understand Public Safety's need for true interoperability, i.e., the ability to communicate without regard for which carrier is used by which agency, and the ability to seamlessly roam and use any

equipment on any network. Although we see the word “interoperability” used extensively, true interoperability does not mean it only applies to users on only one network.

History of FirstNet:

Although the concept of Public Safety Broadband has a long history, the FirstNet project was officially begun in 2012, via Public Law 112-96, the “Middle Class Tax Relief and Job Creation Act of 2012”, (a.k.a. the “Act”) to provide a broadband cellular network that would meet the needs of Public Safety. As part of the act, the First Responder Network Authority, a.k.a. FirstNet was established to implement and operate the network. The act provided funding and spectrum, known as “Band 14 to FirstNet to be able to build the network.

The law requires the network to use LTE as its network standard (47 USC 1423 (c) (2)). LTE is an international standard, developed and maintained by 3GPP. LTE is used in cellular networks worldwide, and is considered the de facto standard. The FirstNet network is intended to provide high speed service with high availability, priority and preemption for Public Safety users, high capacity, and very importantly, ability to allow for interoperability with commercial networks.

In the early days of FirstNet, based on the knowledge of the technology before 2012, it was thought by most that an independent network was going to be built from the ground up. We believe that the realization that Public Safety did not need yet another communications silo was the reason that the law includes language about making connections to commercial networks. (For example, 47 USC 1426 (c) (5), Roaming Agreements, and 47 USC 1431 Public safety roaming and priority access)

As time went on, it was realized that it would be much more financially efficient to use an established commercial network provider’s infrastructure as the basis for the network.

In fact, the Act requires the use of commercial infrastructure, 47 USC 1426 (b) (1) (C): “...encouraging that such requests leverage, to the maximum extent economically desirable, existing commercial wireless infrastructure to speed deployment of the network...”

In 2016, FirstNet awarded the contract to AT&T and their partners to provide service nationwide for the FirstNet network. Not only does AT&T intend to support Public Safety service users on Band 14 alone, they have stated that they intend to provide FirstNet service using all of AT&T’s spectrum bands. Basically, AT&T fully followed the intent of the law by not only using their physical infrastructure, (towers, sites, backhaul, etc.), but by also using the entirety of their spectrum infrastructure. This promises to provide Public Safety with an enormous amount of capacity, when needed, compared to restricting FirstNet to the use of Band 14 alone.

AT&T showed that a carrier can provide FirstNet-level service across any spectrum and network by:

- a. Following the applicable 3GPP standards for LTE that pertain to Public Safety use.

- b. Applying hardening, enhancing coverage, and implementing all the other requirements in the RFP / Contract with FirstNet.
- c. Using any frequency band that they have available, not just Band 14.

Discussion

By law, the FirstNet network must follow the LTE standards as developed by the 3GPP standards body. This is a good thing, as LTE is a worldwide, as well as a nationwide standard, and is used by all carriers in the United States. And priority and preemption, MC-PTT, and other supporting functionality are (or will soon be) part of the 3GPP standards for LTE. Any carrier could provide these services by implementing these features based standards on their network(s).

FirstNet has always promoted competition as an effective way to allow the private sector to innovate; their RFP used the competition in the technology marketplace to come up with a solution that appears able to meet most of the very demanding needs of First Responders.

Competition is the best method to drive innovation and lower pricing. We believe that there are other carriers that should be able to provide Public Safety grade service with LTE standards based priority and preemption. However, statements from both FirstNet and AT&T have indicated that connections that maintain prioritization between networks will not be allowed. This gets us perilously close to a government sanctioned monopoly, where we have an arbitrary restriction on prioritized access that we do not believe is based on a limitation in technology.

There are a number of valid reasons why a Public Safety agency would want to have a choice in which carrier supplies their service: features, functions, pricing, wireless coverage in their jurisdiction, backup & redundancy, and others.

The CPSBGB noted that the current approximate Public Safety cellular market share in Colorado is: Verizon 65%, AT&T 15%. Even if the market share were evenly distributed among all carriers providing prioritized Public Safety Service, it is unlikely that even a majority of Public Safety users would be moved to FirstNet for several years, at least.

It is unrealistic to expect that every single Public Safety agency would voluntarily move their broadband cellular operations to a single carrier, especially considering that these networks, especially outside the cores, are built to commercial standards and serve commercial, retail customers. Had the initial concept of FirstNet being built as a stand-alone, purpose-built Public Safety network come to fruition, the case could have been made for all Public Safety to move to that network. However, as we have seen, this would have been a prohibitively expensive, and time consuming project. The end result of a commercial carrier winning the contract to supply the network service was, in the end, a reasonable tradeoff between cost efficiency and a 100% purpose-built network.

In today's world, Public Safety agencies can and do use various carriers to provide their cellular service. Since Public Safety cellular service has not been on a priority basis (until recently), it really doesn't matter which carrier is used. Information passed between Public Safety agencies on different carrier networks is carried through gateways in the same manner as commercial traffic, so priority & preemption does not exist at any point in the process.

With FirstNet using updated LTE 3GPP standards, and other carriers being able to use those same standards, Public Safety users can use priority and preemption within whichever network they happen to be using. However, it's our understanding that the prioritized traffic loses its QPP designation when moving between different carrier networks. This means that when adjacent agencies on different networks are trying to communicate during an emergency, information sent from agency A to agency B will be treated as just normal commercial traffic both on the connection between networks, as well as on the other carrier's network.

In the matter of cellular MC-PTT, we have similar concerns with isolated networks and the silos they create.

As it stands today, PTT communications that use 3GPP LTE standards supplied by a given carrier would not cross network boundaries, unless individual agencies invest in additional interoperability equipment to connect specific talkgroups between specific agencies.

A similar situation exists with over-the-top PTT applications. While they can communicate across carriers, they suffer from the same loss of priority between networks described above. And these applications cannot communicate with another similar PTT applications, requiring added interoperability equipment.

The requirement to use additional interoperability equipment adds additional cost, complexity, and additional points of failure to what is arguably the most critical communications method for emergency responders. Additionally, this will not help in the event of a large scale emergency, as agencies from outside the area most likely are not included in the original interoperability system.

These are serious issues for Public Safety, as we should not have to worry about who is using which carrier. We need to communicate seamlessly when the lives and property of our citizens are at stake.

Which leads us to the area of Interoperability. We are seeing the term bandied about with no regard as to what this term really means. For the purposes of this request, we use the SAFECOM definition of interoperable communications, as it is based on the needs of Public Safety communications:

"The ability of Public Safety responders to share information via voice and data communications systems on demand, in real time, when needed, and as authorized."

There is no mention of proprietary systems, market share, etc. The definition of interoperability requires that communications be able to occur regardless of who is using what manufacturer's equipment, or which carrier's network. The idea that a carrier provides interoperability – but only to users on their network - doesn't really meet the definition as stated above.

In our reading of 47 USC 1431 (see above), it is very apparent that Congress intended FirstNet to be interoperable with other carrier networks. This is especially important to maintain priority and preemption settings when information is passing between carrier networks, as well as allowing Public Safety MC-PTT traffic to pass unhindered between carriers. (Having priority and preemption available in only one direction, i.e., only from FirstNet to other networks, is counterintuitive and does not seem to fit the intent of the law.)

Even though the vision of the network has changed from a purpose-built network to a modification of an existing commercial network to provide FirstNet service, we do not believe that this changes the need for the ability to seamlessly communicate with priority and preemption between the various commercial networks and FirstNet. In fact, since the FirstNet network is basically a modified commercial network instead of 100% purpose-built, we believe that this need is even greater.

We believe that the law intended that proprietary networks, and concerns about business advantage & market share, not be an issue when Public Safety is working to protect lives and property.

Scope of Proposed Rulemaking

We request the Commission develop rules that address four major issues that we foresee limiting the future usefulness of cellular broadband for Public Safety:

1. The ability of First Responders from different agencies to communicate while retaining their QPP designations, between any interested carrier's networks. If carriers do not wish to supply this type of service, they would not be required to, and these rules would not apply to them. These rules would address prioritized Public Safety Core to Public Safety Core connections, either full-featured connections or connections set up for specific types of communications. Currently, the position of FirstNet and their vendor seems to be that if Public Safety wants to be able to communicate seamlessly in this manner, then everyone must switch to the FirstNet network. We see this as an unacceptable position, which is reminiscent of the LMR shortcoming where every radio system was/is a silo. This is simply not a position Public Safety wants to experience again.
2. To support full and true interoperability, Mission Critical Push to Talk (MC-PTT) communications should be seamless between users on any carriers supplying MC-PTT service. A user on a carrier supplying MC-PTT service that follows the applicable 3GPP LTE standards should be able to communicate seamlessly via MC-PTT to another user on another network that is also following the applicable 3GPP LTE MC-PTT standards. The fact that two responders from different agencies are using two different carriers for MC-PTT should be invisible to the users. Similar to above, if a carrier does not wish to supply Public Safety 3GPP LTE MC-PTT service, it would not be required to, and these rules would not apply. We would also encourage similar interoperability between Public Safety users on

differing Over-The-Top PTT applications, if they are to be used as a Mission Critical PTT service.

3. A First Responder device, using FirstNet or any other carrier's service, should be able to freely and seamlessly roam between networks as necessary, and where allowed by Public Safety Agency policy. We note that the technology is maturing to the point where this is now possible. Devices that can operate on all US cellular bands, multi-SIM devices, and e-SIM technology are all becoming available to enable devices to operate on any carrier network. There are numerous reasons for seamless roaming, a given carrier's network could be out of service or impaired; the device may have moved into an area where coverage is better on another network; or a variety of other technical, administrative, or operational reasons. We again refer to the LMR world where it is common to have a given radio programmed to use a multitude of systems. Again, if a carrier does not supply Public Safety services, these rules would not apply to them.
4. The Commission should develop any other rules that encourage competition on a level playing field. Concern exists that having only one carrier network as the designated Public Safety provider, with restrictions on prioritized Public Safety access from other networks, will have unintended consequences, especially when First Responders from other networks are not allowed to communicate seamlessly while using all possible features between differing networks. Examples such as dropped calls and lost information in an emergency situation immediately come to mind. Additionally, as stated earlier, competition is the driver behind innovation and produces constant downward pressure on costs.

We believe that for cellular broadband services to be truly useful, especially during disasters and major events, and truly embraced by Public Safety, this type of interoperability is absolutely essential, especially in the areas of mission critical Video and MC-PTT.

Video streams are very sensitive to network congestion, which causes packet delays, jitter, and other timing issues. Real-time streaming video requires that packets arrive on time and in the order they were sent. If timing issues occur, the received video quickly starts to degrade, suffering pixelating, video dropouts, and ultimately the complete loss of video. Timing issues can occur anywhere in the path from the sender and receiver. If the video is being communicated over one QPP enabled network, there would be few issues. However, if QPP designations of the packets are lost as the video passes between networks, we anticipate that video streams could quickly be degraded. The ability to communicate over multiple QPP enabled networks means that video would be a reliable, robust tool for all sorts of incidents and events.

This is also true in the area of Mission Critical Push to Talk (MC-PTT), as voice packets are also very vulnerable to delays and jitter. Timing problems can quickly make a voice transmission unreadable and essentially useless.

Among the multitude of issues that would need to be solved to make MC-PTT a reliable option would be the fact that under the current model, reliable and seamless MC-PTT between carriers would not occur. There are two basic forms of MC-PTT service that are available today that we need to consider:

1. “Over-The-Top” PTT services are carrier-independent, may or may not be 3GPP compliant, and they are treated as any other data on the network and on the connections between networks. Since there is no current method to prioritize data between networks as described elsewhere, critical PTT communications would be non-prioritized when users are communicating between networks. This has serious implications for differing agencies using different carriers. Those PTT communications that become “un-prioritized” when leaving the originating network could very likely become unreliable as they enter another network.
2. Embedded PTT services are generic to the individual carrier’s networks, and in the future would be most likely based on 3GPP standards. Currently, these types of PTT services are not interoperable between carriers, unless added infrastructure is provided to bridge a specific talkgroup(s) between carriers. Having to use an added method to bridge talk paths is technically clumsy, adds an unnecessary layer of complexity, as well as an additional point of failure, (which, of course, can fail at the worst possible time). Requiring MC-PTT communications to cross network boundaries in a seamless manner is going to be a necessity if we expect cellular PTT to be able to supplant traditional LMR networks in any meaningful way.

Both embedded and over the top PTT services should be able to seamlessly interoperate if they are intended to be used in a Mission Critical PTT environment.

We are not specifically advocating for the requirement of direct core-to-core connections, or any other technical method for that matter. Our only interest is the ability of Emergency Responders to communicate seamlessly across networks, i.e., not having to worry about who is using what network.

However, we are not convinced that connecting two or more Public Safety Cores from differing carriers is unattainable due to security concerns. We observe that FirstNet appeared to anticipate the need for core to core connections between carriers in their RFP, at least at some level.

Specifically, the FirstNet RFP addresses connections to other carriers and entities, and we would hope these RFP requirements are included in the contract with FirstNet’s vendor (although we have no way to verify this one way or the other, as FirstNet’s contract with their vendor has not been made available to the public, nor potential FirstNet users). These requirements are spelled out in Section J, Attachment J-4 System and Standard Views. The RFP addresses two types of connections, 5 Roaming Interface [Interface #3], and 6 MVNO Interface [Interface #4]. FirstNet clearly anticipated the need for connections between carriers, and listed in great detail all the applicable 3GPP and other standards to be followed when making these types of connections.

Indeed, all the major carriers in the US have roaming agreements with numerous roaming partners, or support the operations of multiple Mobile Vehicle Network Operators (MVNO). Additionally, our understanding is that FirstNet's vendor will be providing Public Safety service to some areas of the US via their roaming partners. As far as we can see, based on the successful operations of these arrangements, and the seeming lack of security issues, connections between cores appear to be a viable method.

However, we are not experts in the design and operation of LTE carrier networks. And, we do not pretend to be able to dictate the explicit rules that are required to assure that Public Safety receives service in the most expeditious, reliable, and efficient manner possible. But we do know, based on past experience that the issue of seamless First Responder communications across differing carrier networks will not get better without all the players working toward a common goal of interoperability. Without a regulatory framework, it is our opinion that this is unlikely to occur on its own. It is absolutely imperative that the rulemaking process be started as soon as possible to avoid future problems that will only compound over time.

We realize that this will be no easy undertaking, and will require input from all stakeholders in order to identify solutions that will work the best for everyone. There will be a host of questions that would need to be answered, including (but not limited to):

- Does every carrier follow FirstNet's standard for First Responder eligibility?
- Will there be a set of standards that will apply to any carrier that wishes to provide Public Safety services, i.e., site hardening, redundancy, required availability metrics, etc.?
- Have networks wishing to provide Public Safety service sufficiently hardened their infrastructure in its entirety?
- How would a carrier be "certified" or otherwise proven to be following 3GPP Public Safety standards, and who would perform this function?
- How would compliance with standards be enforced, and by who?
- Would a carrier offering Public Safety service be required to use a separate dedicated core to provide that service?
- What defines a dedicated, isolated "Public Safety Core"?
- Are all Public Safety carriers required to move to the 3GPP LTE Standards release in the same timeframes?
- How will this affect cyber security?
- Does connecting dedicated Public Safety Cores help mitigate, or aggravate, security risks?
- How can we quarantine a cyberattack from spreading through all the networks?
- What types of traffic are universally considered worthy of priority and preemption across all networks?

We believe that both the current level of technology and the 3GPP LTE standards support these types of rules, that is, no new technology will need to be developed - we will just need to apply what already exists.

Conclusion

We encourage the Commission to act proactively and swiftly to ensure that Public Safety is able to make the best use of LTE technologies, without regard to manufacturers and vendors, by being able to use whichever Public Safety broadband service that meets their needs. Most importantly, the choice of which Public Safety LTE provider to use should not mean that a Public Safety agency needs to decide if they wish to have interoperability or not. In the LMR world, it has taken decades for interoperability to reach its current state. In retrospect, based on the lessons we've learned, it would have been a much easier road had the Commission had rules in place that mandated interoperability that is independent of manufacturer or supplier.

We also understand that the Commission might be reluctant to conduct rulemaking on this issue, believing that a more hands-off posture may be more appropriate, and not wanting to overregulate the issue. However, we are not concerned that the Commission's rules in this respect would damage the ability of any carrier to operate and provide Public Safety service. In fact, we believe that the Commission would be able to develop rules that would enhance Public Safety use of cellular networks. After all, the Commission currently regulates today's US cellular marketplace, and by all measures, it is very healthy and innovative.

We suggest that the level of LTE technology, and the current development of the 3GPP standards provide a platform to enhance interoperability between any Public Safety agency and any carrier. We should all be considering interoperability as simply another feature that is basic to any communications network. We should not be forced into a situation where we are being told that communications silos are necessary, that Public Safety and their mission to safeguard our citizens are simply secondary to contracts, competitive advantage, and business secrets. We understand the requirement for carriers to be profitable, and carry out their fiduciary duty to their shareholders. We recognize that stable, financially healthy carriers benefit Public Safety.

However, what must also be understood is that Public Safety has a duty to safeguard our citizens, and seamless interoperable communications across all platforms is vitally imperative to fulfil that duty. We simply cannot subordinate the protection of life and property to be secondary to business concerns.

We urge the Commission to act quickly on this matter, and consider the comments and positions of all the stakeholders involved in this issue.

Sincerely,

The Illinois Public Safety Broadband Working Group